VIRGINIA LAW REVIEW
IN BRIEF

VOLUME 97 MARCH 20, 2011 PAGES 1–12

RESPONSE

MASSIVE HARD DRIVES, GENERAL WARRANTS, AND THE POWER OF MAGISTRATE JUDGES

Paul Ohm[*]

MOST legal scholars who write at the intersection of technology and the Fourth Amendment spend much of their time building upon Professor Orin Kerr's many clear and insightful articles, and I am no exception. It is thus with great respect and deference that I explain what Professor Kerr gets wrong in his latest article, *Ex Ante Regulation of Computer Search and Seizure*.[1]

In *Ex Ante Regulation*, Professor Kerr tries to disrupt a trend emerging from the lower federal courts: the imposition by magistrate judges of limits on what the police can do with a search warrant for digital evidence stored on computer hard drives. These judges have tried to impose a diverse set of requirements and restrictions on these warrants—catalogued by Professor Kerr—such as limits on how long the police can retain a computer and what they can do when they examine its hard drive.[2]

[*] Associate Professor, University of Colorado Law School. I thank Jennifer Granick, Lee Tien, Blake Reid, and Magistrate Judge Stephen Smith for their comments and Janna Fischer and Nicole Friess for their research assistance. My thoughts about the *Comprehensive Drug Testing* decision were shaped through earlier conversations with Nicole Friess, Bert Lao, Devin Loojien, Jennifer Lynch, and Jason Wu. Finally, I thank Orin Kerr, my mentor and friend, for his comments and for giving me plenty to write about.

[1] 96 Va. L. Rev. 1241 (2010).

[2] Id. at 1248–60.

Professor Kerr offers both doctrinal and normative arguments against ex ante search warrant restrictions.[3] His doctrinal arguments are the more provocative ones: he thinks ex ante warrant restrictions like these are lawless acts, beyond the constitutional and statutory power of magistrate judges. I disagree, and in this Essay, I respond almost entirely to these arguments, because if they are correct, then a normative debate is almost beside the point.[4]

For support, Professor Kerr points to four Supreme Court cases which, as he concedes, "[v]iewed in isolation . . . do not definitively rule out the lawfulness of ex ante restrictions on the execution of computer warrants," but which he claims, "[t]aken together . . . undercut every aspect of the lawfulness of such restrictions."[5] I respectfully disagree. Two of the cases are easy to distinguish, as Professor Kerr seems to concede.

First, *Lo-Ji Sales v. New York*,[6] in Professor Kerr's words, "presents the extreme case of a magistrate judge controlling the execution of the warrant by participating in the search."[7] The magistrate judge in *Lo-Ji Sales*, who sat at the scene of a search ruling on what could and could not be seized, presents a dramatically more involved figure than a judge sitting in chambers refusing to sign a computer search warrant for failing to specify a search protocol "designed to uncover only the information for which [the government] has probable cause."[8]

The need for such a search protocol was suggested by Chief Judge Kozinski of the Ninth Circuit, in a concurring opinion, in a case called

[3] Professor Kerr doesn't dislike restrictions on search warrants only in the computer search context. He recently cited *Ex Ante Regulation* on his blog to criticize a Magistrate Judge's decision to find a protectable Fourth Amendment interest in the historical records of where a person's cell phone had traveled. Orin Kerr, Fourth Amendment Stunner: Judge Rules That Cell-Site Data Protected by Fourth Amendment Warrant Requirement, The Volokh Conspiracy (Aug. 31, 2010), http://volokh.com/2010/08/31/fourth-amendment-stunner-judge-rules-that-cell-site-data-protected-by-fourth-amendment-warrant-requirement/.

[4] I disagree with Professor Kerr's normative assessment as well, but I will save that disagreement for another day.

[5] Kerr, supra note 1, at 1270.

[6] 442 U.S. 319 (1979).

[7] Kerr, supra note 1, at 1262.

[8] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1180 (9th Cir. 2010) (en banc) (Kozinski, J., concurring) [hereinafter *CDT II*].

United States v. Comprehensive Drug Testing (*CDT II*),[9] an opinion that bears a fair amount of Professor Kerr's criticism.[10] Judge Kozinski advised that a "warrant application should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown."[11] Not only does this reasoning not contradict *Lo-Ji Sales*, but also it seems designed to protect against what the Supreme Court criticized in that case—that "the warrant left it entirely to the discretion of the officials conducting the search to decide what items were likely obscene and to accomplish their seizure. The Fourth Amendment does not permit such action."[12]

Second, *Dalia v. United States*[13] is also not very instructive, as Professor Kerr concedes, because "[the defendant] argued that a restriction on the method of executing the warrant was *required*, not that it was permitted."[14] This concession seems important because Professor Kerr is using the case to explain why ex ante requirements aren't permitted, not just that they aren't required. On the question of permission, the Court seems to suggest the opposite of what Professor Kerr concludes; in a closing footnote, the Court encourages warrant applications that reveal, ex ante, the method of execution, saying, "[a]lthough explicit authorization of the entry [into an office to

[9] Id. at 1178–80. At the time Professor Kerr wrote his article, Judge Kozinski's opinion stood as the majority opinion of the en banc court, and the search protocol requirement (along with four other requirements) represented a binding rule. 579 F.3d 989, 1006 (9th Cir. 2009) (en banc) [*CDT I*]. After the Justice Department asked for reconsideration, Judge Kozinski lost the majority for these mandatory rules, which became relegated to mere "guidance" in a concurring opinion joined by four other Ninth Circuit judges. *CDT II*, 621 F.3d at 1179–80.

[10] E.g., Kerr, supra note 1, at 1277 (disagreeing with Judge Kozinski's opinion about the proper role of ex ante warrant restrictions).

[11] *CDT II*, 621 F.3d at 1179. Judge Kozinski provided four other pieces of "guidance" for judges faced with warrants for computer search warrants. Whenever the police seek a warrant to search a computer, they should (1) waive the plain view rule, meaning they must agree not to use evidence of crimes other than the one under investigation that led to the warrant; (2) wall off the forensic experts who search the hard drive from the agents investigating the case; (3) explain the "actual risks of destruction of information" they would face if they weren't allowed to seize entire computers; (4) use a search protocol to designate what information they can give to the investigating agents; and (5) destroy or return nonresponsive data. Id. at 1180.

[12] Lo-Ji Sales v. New York, 442 U.S. 319, 325 (1979).

[13] 441 U.S. 238 (1979).

[14] Kerr, supra note 1, at 1266 (emphasis in original).

install a bug] is not constitutionally required, we do agree . . . that the 'preferable approach' would be for Government agents in the future to make explicit to the authorizing court their expectation that some form of surreptitious entry will be required to carry out the surveillance."[15] Not only is the Supreme Court implicitly endorsing the ex ante disclosure of search methods, but also it calls this the "preferable approach."

The two other cases cited by Professor Kerr, *United States v. Grubbs*[16] and *Richards v. Wisconsin*,[17] similarly fail to prove his argument, but explaining why requires a bit more discussion. Crucially, we must identify the part of the Fourth Amendment that ex ante computer search warrant restrictions serve to protect. The Amendment gives at least three possibilities, requiring warrants to (1) be based "upon probable cause"; (2) particularly describe the "place to be searched, and the persons or things to be seized"; or (3) requiring searches and seizures to be "reasonable."[18] Professor Kerr thinks that ex ante restrictions on computer search warrants are only about reasonableness. In contrast, I think they are designed to cure the *manifest lack of probable cause and particularity* in almost every computer case.

If I am right and Professor Kerr is wrong about the source of these restrictions, then Professor Kerr's argument loses most of its force. Outside the computer context, magistrate judges regularly impose ex ante restrictions on search warrants in order to ensure probable cause and particularity. No magistrate judge would sign a warrant to search two houses supported by an application that sets out probable cause to search only one, because such a warrant would suffer from the failure of both probable cause and particularity. Similarly, magistrate judges will often tell a prosecutor to freshen his or her evidence to avoid staleness, or to be more specific in the description of things to be seized. Professor Kerr acknowledges the propriety of ex ante restrictions like these, explaining that the "ex ante assessment of probable cause and particularity serves a different function than ex ante assessment of how a search should be executed."[19]

[15] *Dalia*, 441 U.S. at 259 n.22.
[16] 547 U.S. 90 (2006).
[17] 520 U.S. 385 (1997).
[18] U.S. Const. amend. IV.
[19] Kerr, supra note 1, at 1290–91.

Unfortunately, judges who impose ex ante restrictions on computer searches too often fail to identify what requirement of the Fourth Amendment their rules are meant to uphold. Even Judge Kozinski spends precious little space explaining the legal source for his guidance. I will fill in the missing analyses, explaining why rules like the *CDT II* rules are necessary to compensate for the lack of probable cause and particularity—not merely to ensure reasonable execution—in almost every computer case.

Judges faced with search warrants for computers confront the commingling problem—namely, should the police be allowed to seize and search through many innocent documents for which they lack probable cause in order to find a much smaller number of documents that contain evidence of a crime? In the pre-computer age, judges allowed some forms of over collection as a constitutional compromise, recognizing the proliferation of business records and the practical realities of policing. In these cases, they let the police haul entire filing cabinets containing evidence commingled with innocent material back to the station, permitting them to view every document, separating the relevant from the irrelevant.[20] Judges have permitted this procedure for filing cabinets not necessarily because the Constitution has demanded they do so, but because they have considered it an acceptable compromise, one which adequately balances Fourth Amendment privacy interests against the need of the police to solve and deter crime.

As the world shifts from paper and cabinets to data and computers, we must ask whether the filing cabinet solution continues to strike the proper balance. Many judges have too quickly concluded it does by drawing a facile analogy: computer hard drives full of folders and documents are like filing cabinets full of folders and documents. If the police can haul away a filing cabinet for later, comprehensive search at the station, they should be allowed to do the same thing with a file server.

[20] In an earlier article, Professor Kerr considered the filing cabinet analogy and seems to have concluded that it is useful but imperfect. Compare Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 550 (2005) (acknowledging the usefulness of treating a computer like a container), with id. at 556 (embracing "virtual file" and "exposed information" analogies for computer forensics, which seem to depart from filing-cabinet-derived rules).

The analogy, however, ignores the significant differences between filing cabinets and hard drives, differences that disrupt the careful constitutional balance represented by the filing cabinet solution. Hard drives store more information about more people of a more sensitive nature than filing cabinets ever have; the comparisons aren't even close.[21] In 2005, Professor Kerr noted that hard drives sold at the time "generally [had] storage capacities of about eighty gigabytes," which could hold an amount of text roughly equal to the amount of "information contained in the books on one floor of a typical academic library."[22]

Today, a mere six years later, many computers ship with one *terabyte* hard drives, holding about twelve times more information than those considered by Professor Kerr. His analogical, low slung, one-story academic library building has been replaced by an imposing library tower. Soon, as hard drives continue to grow rapidly, libraries will no longer seem a fitting analogy. By some estimates, the Library of Congress—the largest library in the world—contains ten terabytes of information,[23] the amount of data a typical home computer will store within the next decade.[24]

Of course, the increasing size of hard drives matters only if people are filling these drives with more information than they did before. If on the other hand computer users are merely filling their massive drives with bloated computer programs and copies of television shows while keeping approximately the same number of word processing files, email messages, and photos—the stuff of potential evidence—that they always have in the past, then the growth of disk capacity may not trigger a constitutional concern.

---

[21] The *CDT II* majority opinion summarizes the problem well: "Government intrusions into large private databases thus have the potential to expose exceedingly sensitive information about countless individuals not implicated in any criminal activity, who might not even know that the information about them has been seized and thus can do nothing to protect their privacy." *CDT II*, 621 F.3d at 1177.

[22] Kerr, supra note 20, at 542.

[23] John H. Jessen, An Overview of ESI Storage & Retrieval, 11 Sedona Conf. J. 237, 237 (2010). But see Matt Raymond, How 'Big' is the Library of Congress, Library of Congress Blog (Feb. 11, 2009), http://blogs.loc.gov/loc/2009/02/how-big-is-the-library-of-congress/ (criticizing estimates like these, suggesting that they significantly underrepresent the amount of information in the Library).

[24] If we assume, as Professor Kerr has, that hard drive capacity doubles every two years, Kerr, supra note 20, at 542, then today's one terabyte hard drives will give way to ten terabyte hard drives in 6.6 years.

The former seems to be the case; people produce and retain personalized digital information at a rapidly increasing rate. Vacationers marvel at the thousand-plus digital photos they now take on a week's trip, several orders of magnitude more than when they used to buy film by the roll. And when they return home, most vacationers keep every photo, because culling the bad from the good isn't worth the effort now that disk storage is so cheap. Photos aren't the only things we hoard: we keep music collections whose pre-Internet jewel boxes would have lined many rooms full of shelves, and we increasingly collect many gigabytes of digital home videos and ebooks.

We also store communications like never before. When Google launched its email service in 2004, it startled many by offering one gigabyte of storage, hundreds of times more than was being offered by its competitors, famously bragging that Gmail "users should never have to . . . delete a message."[25] Websites that publish user-generated content have turned many of us into amateur documentarians (YouTube), newspaper headline writers (Twitter), and public diarists (Facebook), and they and we are storing copies of everything we produce. Even when we aren't hoarding, our computers are, with our web browsers remembering every website we visit, storing the addresses in history and copies of the pages themselves in cache.

As if this weren't enough, we now share our computers with other people. Every modern operating system encourages sharing by enabling separate logins and personalization, thereby commingling on one hard drive the evidence of the crimes of the father with the innocent files of the son. The latest Internet trends greatly exacerbate the problem, as many websites are now storing our information "in the cloud," commingling our email messages, word processing documents, voice mail messages, and business data on shared servers alongside the data of "innumerable strangers."[26] As the *CDT II* court put it, "[s]eizure of, for example, Google's email servers to look for a few incriminating messages could jeopardize the privacy of millions."[27]

[25] Press Release, Google, Google Gets the Message, Launches Gmail (April 1, 2004), available at http://www.google.com/press/pressrel/gmail.html.

[26] *CDT II*, 621 F.3d at 1176.

[27] Id.

Finally, the filing cabinet analogy fails to capture the sensitive nature of the data we now store. We tell our Facebook "friends" secrets we once would have shared with only a few close friends, and we reveal health symptoms to Google's search engine that we once wouldn't have bothered to tell our doctors. Our computers track what we read, buy, where we go, and increasingly, what we think. Privacy scholars have argued that criminal procedure law should develop special rules to take into account the now routine storage of evidence of our intellectual lives.[28]

In essence, Professor Kerr's 2005 comparison—"every computer is akin to a vast warehouse of information"[29]—already seems quaint. Warehouses—and even less so filing cabinets—are insignificant containers of information compared to today's hard drives, and the analogy will only become more mismatched over time. As the filing cabinet analogy fails, it takes with it the careful balance of the filing cabinet solution—haul it all away now and sort later. Today's technology poses a constitutional puzzle that is different in kind, not just in degree, from the one solved only a few decades ago.

Ultimately, the irony of Professor Kerr's argument is that a court that agrees with it might feel compelled to *reject wholesale* most search warrants for computers. Deprived of the power to creatively superintend computer searches, a court can reasonably conclude that evolving technological realities leave it no choice but to reject every computer warrant for a manifest lack of probable cause and intractable failure of particularity. Of course, no court would embrace such a stark result, which means courts are likely to reject Professor Kerr's binary, reject-or-approve conception of the Fourth Amendment. Instead, courts will turn to subtler, more nuanced approaches, approving only those warrants that safeguard against the special probable cause and particularity problems of computer searches, namely warrants that contain protections like the *CDT II* rules.

[28] Neil M. Richards, Intellectual Privacy, 87 Tex. L. Rev. 387, 433 (2008) (considering the impact of government surveillance on what he calls "Intellectual Privacy"); Daniel J. Solove, The First Amendment as Criminal Procedure, 82 N.Y.U. L. Rev. 112, 159 (2007) (arguing that criminal procedure should take into consideration the important First Amendment values implicated in today's modern search and surveillance).

[29] Kerr, supra note 20, at 542.

Once we properly understand the *CDT II* rules, and others like them, to be about particularity and probable cause, not reasonableness, Professor Kerr's third Supreme Court case fades away. *Richards v. Wisconsin*[30] construes the knock-and-announce requirement, a rule rooted in the reasonableness clause of the Fourth Amendment,[31] and one which has nothing to do with probable cause or particularity. *Richards* stands only for the proposition that some reasonableness considerations—specifically whether knocking and announcing will risk harm to the police or destruction of evidence—should be weighed at the time the warrant is executed, not at the time it is issued.[32] Nothing in *Richards* suggests in the slightest that ex ante restrictions intended to ensure probable cause and particularity can be ignored.

This leaves Professor Kerr with only one case, *United States v. Grubbs*,[33] for support. But *Grubbs*, too, does not control. *Grubbs* seems to have been an easy case for the Court. It involved an anticipatory warrant: a warrant obtained before the police had probable cause using an application that specified the condition that was expected to occur that would establish probable cause. By the time of the court challenge, however, probable cause was no longer in doubt; at the time the anticipatory warrant had been served, the future condition—the delivery of a package containing child pornography—had occurred,[34] and the Court was asked to decide only whether the police had erred by not leaving a copy of the affidavit with the person whose home had been searched.[35] The Court ruled that the police had not erred, in a short, terse decision which we should try to avoid reading too much into.

Professor Kerr rightly points out, however, that the Court's opinion offers a narrow interpretation of the Fourth Amendment's particularity requirement, holding that "[t]he Fourth Amendment . . . does not set forth some general 'particularity requirement.' It specifies only two matters that must be 'particularly describ[ed]' in the

[30] 520 U.S. 385 (1997).

[31] Wilson v. Arkansas, 514 U.S. 927, 934 (1995) ("[W]e hold that in some circumstances an officer's unannounced entry into a home might be unreasonable under the Fourth Amendment.").

[32] 520 U.S. at 395–96.

[33] 547 U.S. 90 (2006).

[34] Id. at 93.

[35] Id. at 93–94.

warrant: 'the place to be searched' and 'the persons or things to be seized.'"[36] If search protocols for computer searches serve only to satisfy "some general particularity requirement," then *Grubbs* might militate against them.

There are two reasons to reject this reading. First, as described above, magistrate judge-imposed restrictions on search warrants protect against not only the failure of particularity but also the manifest failure of probable cause. But, second, even were a court to decide that the *CDT II* rules were about only particularity and not probable cause, then *Grubbs* still should not control, because the particularity clause should be read differently for computer search warrants, because of the rule against general warrants. The Supreme Court has repeatedly explained that the Fourth Amendment's particularity requirement arose, at least in part, from the founders' concerns about British writs of assistance, general warrants issued by the king permitting soldiers to look in homes and places of business with few restrictions.[37] When something approaches the breadth and level of invasiveness of a colonial era general warrant, the particularity requirement must prohibit it.[38]

Many government practices have been compared to general warrants, but almost none are close to being as invasive as a months-long trawl through a person's personal computer. In *Lo-Ji Sales v. New York*, the Court found a relatively orderly six hour search through an adult bookstore in the presence of the suspect to be "reminiscent of the general warrant or writ of assistance of the 18th

[36] Id. at 97.

[37] Minnesota v. Dickerson, 508 U.S. 366, 378 (1993) ("Where, as here, 'an officer who is executing a valid search for one item seizes a different item,' this Court rightly 'has been sensitive to the danger . . . that officers will enlarge a specific authorization, furnished by a warrant or an exigency, into the equivalent of a general warrant to rummage and seize at will.'") (quoting Texas v. Brown, 460 U.S. 730, 748 (Stevens, J., concurring)); Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("The manifest purpose of this particularity requirement was to prevent general searches."); Steagald v. United States, 451 U.S. 204, 220 (1981) ("The Fourth Amendment was intended partly to protect against the abuses of the general warrants that had occurred in England and of the writs of assistance used in the Colonies.").

[38] See Berger v. New York, 388 U.S. 41, 58 (1967) ("The Fourth Amendment's [particularity] requirement . . . repudiated these general warrants and 'makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another.'") (quoting Marron v. United States, 275 U.S. 192, 196 (1927)).

century."[39] The *Lo-Ji Sales* warrant seems to pale in comparison to warrants issued in a typical computer case, at least with respect to the amount, variety, and sensitivity of the innocent information the police are allowed to rummage through.

Likewise, Justice Douglas noted that a warrant authorizing a wiretap of a person's telephone, an act revealing a paltry amount of innocent information compared to that obtained during the search of a typical hard drive, is "no different from the general warrants the Fourth Amendment was intended to prohibit."[40] While a telephone wiretap is limited to a single mode of communication and in time to a few weeks, a computer hard drive can store web browsing logs, email conversations, calendar entries, reading habits, file transfers, consumer purchases, increasingly intimate voice conversations (Skype and Google Voice), and evanescent, water-cooler-style chat (Facebook status updates) for years or maybe even decades.

Computer search warrants are the closest things to general warrants we have confronted in the history of the Republic.[41] This explains why magistrate judges have spent the past decade acting in a way Professor Kerr finds lawless, trying to solve the constitutional commingling problem with new and creative compromises, with district and appellate court judges weighing in as well. Far from acting beyond their constitutional authority, these judges have been searching for a way to protect Fourth Amendment interests while still allowing the police to solve cases. Nothing the Supreme Court has said about the particularity clause, in *Grubbs* or elsewhere, should be considered the end of the discussion, not at least until the Court is faced directly with the special problem of computer searches.

Not only do I disagree with Professor Kerr's conclusion that magistrate judges lack the power to administer the *CDT II* rules, but also, and quite to the contrary, I believe that the *CDT II* rules—or rules like them—have become necessary; they are the only way the courts

[39] 442 U.S. 319, 325 (1979).

[40] Osborn v. United States, 385 U.S. 323, 353 (1966) (Douglas, J., dissenting).

[41] As the *CDT II* majority opinion put it: "This pressing need of law enforcement for broad authorization to examine electronic records, so persuasively demonstrated in the introduction to the original warrant in this case, creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *CDT II*, 621 F.3d at 1176 (citation omitted).

can fulfill their constitutional duty to protect privacy from government overreaching.

* * *

In the government's appeal of *CDT II*, the Justice Department painted the consequences of the now amended en banc opinion in dramatic terms, arguing that the *CDT II* rules "will be grossly inefficient, lead to delays in obtaining time-sensitive evidence, and heighten the risk that important information will be missed."[42] Overheated claims like this demand a response.

I do not doubt the *CDT II* rules would force the FBI to expend more resources on computer forensics; I am sure the burden would be more heavily felt in state and local agencies, which lack the resources of the FBI. But I know enough about computer forensics—having led a task force during my time at the Justice Department that explored the difficulties the FBI was having analyzing hard drives—to know that my former colleagues will rise to the occasion.

It might take more resources, training, and personnel to analyze a hard drive in a world with the *CDT II* rules than without, and evidence and maybe even cases might occasionally be lost, but this would be the price of liberty, privacy, and life in a constitutional system. And I don't believe for a minute that all computer forensics will need to shut down or that a large number of cases will be lost. The FBI and other law enforcement agencies are resourceful organizations full of industrious, creative, intelligent, and hard-working agents, who are dedicated to finding evidence of crime. If the Fourth Amendment imposes new restrictions on what law enforcement agents can do, those agents will, as they have so many times before, find a way to continue to do their jobs efficiently and successfully while at the same time respecting the rights of the people.

[42] Brief for the United States in Support of Rehearing En Banc by the Full Court at 16, United States v. Comprehensive Drug Testing, Nos. 05-10067, 05-15006, 05-55354 (9th Cir. 2010). See also id. at 6 ("Many United States Attorney's Offices have been chilled from seeking any new warrants to search computers.").